國立成功大學
National Cheng Kung University

對稱式密碼系統 補充4

計網中心 網路與資訊安全組

李南逸

National Cheng Kung University

作業4

- 請破解AES加密器產生之密文
  - 請同學將學號最後一碼mod 5，依所得之餘數x，嘗試解出第x組金鑰
    - ■: 尚未得知的密碼

	密文	金鑰
X=0	2mfH5wwaQuC9qvrfFPMgvIvU1ggfGcg8jkanFZfn91k=	@K■X%■3Qh■DD■RqQ
X=1	IZ7J32pjWOR0zpJeQbj1Z+Mu0cRftohz6imCF3+2k1w=	■-?5Q■E■qeDe■%Bs
X=2	Wj3RQTGXWvIeIu5nEt2qYuYbHRhoNtJawk07R0oZWnI=	Hj■N)■tgZ■9wrc■m
X=3	5iPWm3PyGLyk04HUlSSmrJTf9aGSpzferYUyitL8cQ8=	■Y5■V9C96L■X8■8u
X=4	16zvA3lnMuWHoE5PpaJheQ==	s■hv■4z*■7d*t■Ce

作業4

- 加密模式： ECB mode
- 演算法padding方式 : zeropadding
- 演算法運算時使用的編碼格式 : utf-8
- 先將密文從base64編碼格式轉成utf-8格式進行破解，最後再轉成字串查看明文結果
- 範例：金鑰是123456789 ，明文是security，輸出密文是 pKjVPv28yVMn5cRXeUNYpg==

- 繳交
  - 1. Pdf檔案 (內容包含正確密鑰、解出明文、截圖需含moodle姓名、解出畫面)
  - 2. 三週內繳交
  - 3. 一人一組